P●NT COOPERATION TREATY ●

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference J00024868WOA	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/GB 98/01876	International filing date *(day/month/year)* 26/06/1998	(Earliest) Priority Date *(day/month/year)* 26/06/1997

Applicant

BRITISH TELECOMMUNICATIONS PUBLIC L. C. ....et al.

This International Search Report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This International Search Report consists of a total of _____4_____ sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. [ ] **Certain claims were found unsearchable** (see Box I).

2. [ ] **Unity of invention is lacking** (see Box II).

3. [ ] The international application contains disclosure of a **nucleotide and/or amino acid sequence listing** and the international search was carried out on the basis of the sequence listing

     [ ] filed with the international application.

     [ ] furnished by the applicant separately from the international application,

         [ ] but not accompanied by a statement to the effect that it did not include matter going beyond the disclosure in the international application as filed.

     [ ] Transcribed by this Authority

4. With regard to the **title**, [X] the text is approved as submitted by the applicant

         [ ] the text has been established by this Authority to read as follows:

5. With regard to the **abstract,**

     [ ] the text is approved as submitted by the applicant

     [X] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this International Search Report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is:

     Figure No. ____1____ [X] as suggested by the applicant.   [ ] None of the figures.

         [ ] because the applicant failed to suggest a figure.

         [ ] because this figure better characterizes the invention.

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6   H04L29/06   G06F1/00   G06F17/30

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

IPC 6   H04L   G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	STAINOV R: "DATENSICHERHEIT IM INTERNET: PRINZIPIEN, MOEGLICHKEITEN UND GRENZEN" NTZ NACHRICHTENTECHNISCHE ZEITSCHRIFT, vol. 49, no. 8, 1 January 1996, pages 32-34, 36 - 38, 40, XP000623476	9,10,19, 21
A	see page 36, left-hand column, line 4 - right-hand column, line 10 see page 37, right-hand column, line 18 - page 38, left-hand column, line 34; figure 4 see page 40, middle column, line 2 - right-hand column, line 41; figure 5	1,11,15, 23
A	WO 96 42041 A (OPEN MARKET INC) 27 December 1996 see abstract see page 5, line 22 - page 6, line 16 see page 10, line 6 - page 15, line 8	1

-/--

| X | Further documents are listed in the continuation of box C. | | X | Patent family members are listed in annex. |

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
30 November 1998	04/12/1998

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Dupuis, H

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 548 646 A (AZIZ ASHAR ET AL) 20 August 1996 see the whole document -----	22

INTERNATIONAL SEARCH REPORT

Information patent family members

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
WO 9642041	A	27-12-1996	US	5708780 A	13-01-1998
			US	5812776 A	22-09-1998
			AU	694367 B	16-07-1998
			AU	5936796 A	09-01-1997
			CA	2221506 A	27-12-1996
			EP	0830774 A	25-03-1998
US 5548646	A	20-08-1996	EP	0702477 A	20-03-1996
			JP	9027804 A	28-01-1997

line 1, after "server" insert "(AS)"
line 2, after "servers" insert "(APS)"
line 3, after "server" insert "(AS)", after "servers" insert "(APS)"
line 4, after "user" insert "(T1,T2,T3)", after "servers" insert "(APS)"
line 5, after "terminal" insert "(T1,T2,T3)"
line 6, after "server" insert "(APS)"
line 9, after "terminal" insert "(T1,T2,T3)", after "terminal" insert "(T1,T2, T3)"
line 10, after "terminal" insert "(T1,T2,T3)"
line 11, after "server" insert "(APS)"
line 12, after "terminal" insert "(T1,T2,T3)"
line 14, after "server" insert "(APS)"

PAT...I COOPERATION TREATY

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

From the INTERNATIONAL BUREAU

To:

United States Patent and Trademark Office
(Box PCT)
Crystal Plaza 2
Washington, DC 20231
ÉTATS-UNIS D'AMÉRIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 02 February 1999 (02.02.99)	
International application No. PCT/GB98/01876	**Applicant's or agent's file reference** J00024868WOA
International filing date (day/month/year) 26 June 1998 (26.06.98)	**Priority date (day/month/year)** 26 June 1997 (26.06.97)

Applicant

LEVERIDGE, Philip, Charles et al

---

1. The designated Office is hereby notified of its election made:

    [X] in the demand filed with the International Preliminary Examining Authority on:

    24 December 1998 (24.12.98)

    [ ] in a notice effecting later election filed with the International Bureau on:

    _____

2. The election [X] was

    [ ] was not

    made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO 34, chemin des Colombettes 1211 Geneva 20, Switzerland	**Authorized officer** Catherine Massetti
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

DATA COMMUNICATIONS

This invention relates to data communications, and in particular, but not exclusively, to the communication of data via a public data communications network such as the Internet.

5   Due to the inherently insecure nature of data communications via the Internet, and due to the sensitive nature of some information which is transmitted, various proposals have been made for the encryption of data for transmission. Thus, although third parties may be able to intercept messages, third parties will only be able to read the data within the message if they are able to decrypt the message using an appropriate encryption key.

10   In public-key cryptography, such as that used in the RSA cryptography system, each person who is to receive encrypted data has a public key which is made available to anyone wishing to send that person data, and a private key which remains confidential. Data encrypted with the public key can only be decrypted with their private key. This system suffers drawbacks in that, in order to send another party an encrypted message, the sending party must know the

15   public key of the receiving party. Also, the authenticity of the sending party cannot readily be identified since the public key is, by definition, available to any other party.

Another type of encryption system is secret-key cryptography, also referred to as symmetric cryptography. In secret-key cryptography, the sending party and the receiving party share a common secret encryption key, which is used both to encrypt data before transmission,

20   and to decrypt the data after reception. One drawback of this system is that the two parties must, before transmission of the encrypted data, have agreed upon the shared secret key to be used.

A further problem encountered in communications over the Internet is that of the authentication of a user. For example, when a conventional Web server contains premium content documents, the Web server checks a username and password, which must be previously

25   established, transmitted with a document request, each time a premium content document is requested. Many Web pages contain a number of documents (e.g. text files, image files, sound files), for each of which the username and password check is necessary. This password-based authentication procedure is resource intensive, particularly when the user wishes to have access to a large number of documents.

30   In accordance with one aspect of the invention there is provided a method of authenticating a user for access via a terminal connected by an Internet Protocol connection to a Web server, said method comprising:

storing authentication details of authorised users;

performing authentication of a user with reference to said stored authentication details;

transmitting an identifier for the user's terminal to said terminal for storage thereon, the identifier being transmitted in such a manner that the identifier is transmitted by said user terminal with document requests directed at said Web server;

5   storing status data indicating said identifier to be an identifier of a terminal of a currently authenticated user; and

allowing said Web server to access said status data in order to check the authentication status of a user on receipt of a document request containing said identifier.

This aspect allows the transmitted identifier to be used to confirm the authenticated

10   status of the user following an initial password-based authentication check.

The identifier may be transmitted as an HTTP cookie, such that a client browser automatically returns the identifier with any document request directed to a Web server to which the cookie is configured to be returned.

In accordance with a further aspect of the invention there is provided a method of

15   authenticating users for access via terminals remotely connected to a plurality of application servers, said method comprising the steps of:

storing authentication details of authorised users;

performing remote authentication of users with reference to said stored authentication details;

20   storing status data distinguishing users which are currently authenticated from those which are not; and

allowing said plurality of application servers to access said status data to check an authentication status of a user using an identifier for the user's terminal in a service request.

This aspect of the invention provides for the authentification of a user over the Internet

25   using a single authentication facility, which maintains the authentication status of users in the system. When a user wishes to access any of the application servers they may each contact the central facility to confirm the authentication status of that user, without needing to perform separate authentication procedures directly with the user.

In accordance with a further aspect of the invention there is provided a method of

30   transferring a file from a first client terminal to a second client terminal, said method comprising the steps of:

holding file transfer parameters for a plurality of different file transfer types;

transmitting data relating to at least one of said different file transfer types to said first client terminal;

receiving said file from said first client terminal;

receiving data identifying a selected file transfer type from said first client terminal; and

transmitting said file to said second client terminal in accordance with the file transfer parameters stored for said selected transfer type.

This aspect of the invention allows file transfers to be configured without requiring the file transfer parameters to be individually set up by the user at the first client terminal.

Further features and advantages of the present invention in its various aspects will be appreciated from the following description, referring to the accompanying drawings wherein:

Figure 1 is a block diagram schematically illustrating a data transmission arrangement in accordance with the present invention;

Figure 2 is a block diagram schematically illustrating the client/server communications between a client terminal and servers provided in accordance with the present invention;

Figure 3 is a flow diagram illustrating an authentication procedure;

Figure 4 is a block diagram schematically illustrating an authentication response, and session key, generating algorithm;

Figure 5 is a flow diagram illustrating procedures carried out by a server maintaining an updated list of user authentication statuses;

Figure 6 is a flow diagram illustrating further updating procedures carried out by the server maintaining a list of currently authenticated users;

Figure 7 is a flow diagram of authentication procedures carried out by an application server in accordance with a further embodiment of the invention;

Figure 8 is a flow diagram illustrating an authentication status update procedure;

Figure 9 is a block diagram schematically illustrating a file transfer system in accordance with an embodiment of the invention;

Figure 10 is a flow diagram illustrating procedures carried out by a file transfer server;

Figures 11, 12, 13, 15 and 16 are event sequences illustrating client/ server communications;

Figure 14 is a block diagram illustrating a data transmission block in accordance with an embodiment of the invention; and

Figure 17 is a block diagram illustrating a system for transferring e-mails in accordance with an embodiment of the invention.

CLAIMS

CLAIMS:

5   1.   A method of authenticating a user for access via a terminal connected by an Internet Protocol connection to a Web server, said method comprising:

storing authentication details of authorised users;

performing authentication of a user with reference to said stored authentication details;

transmitting an identifier for the user's terminal to said terminal for storage thereon, the

10   identifier being transmitted in such a manner that the identifier is transmitted by said user terminal with document requests directed at said Web server;

storing status data indicating said identifier to be an identifier of a terminal of a currently authenticated user; and

allowing said Web server to access said status data in order to check the authentication

15   status of a user on receipt of a document request containing said identifier.

2.   A method according to claim 1, wherein said identifier is transmitted in an HTTP header to said user terminal.

20   3.   A method according to claim 1 or 2, wherein said authentication step comprises receiving said identifier from said user terminal with an authenticator of the user at said user terminal.

4.   A method according to claim 3, wherein said authentication step comprises issuing a

25   new identifier to said user terminal if said authentication is invalid.

5.   A method according to claim 4, wherein said identifier comprises data indicating the number of times an invalid authenticator has been received from said user terminal.

30   6.   A method according to claim 5, wherein said method comprises issuing no further identifier to said user terminal if an identifier received from said user terminal indicates that a predetermined number of invalid authenticators have been received from said user terminal.

22

7.   A method according to any preceding claim, comprising timing out said identifier as an identifier of a terminal of a currently authenticated user if no document request is received from said user terminal for a predetermined period.

5 8.   A method according to any preceding claim, comprising authenticating said user for access to a plurality of Web servers located in the same Internet domain; and

allowing each of said Web servers to access said status data.

9.   A method of authenticating users for access via terminals remotely connected to a
10 plurality of application servers, said method comprising the steps of:

storing authentication details of authorised users;

performing remote authentication of users with reference to said stored authentication details;

storing status data distinguishing users which are currently authenticated from those
15 which are not; and

allowing said plurality of application servers to access said status data to check an authentication status of a user using an identifier for the user's terminal received in a service request.

20 10.   A method according to claim 9, further comprising producing an encryption key in addition to said status data during said remote authentication step.

11.   A method according to claim 10, wherein said encryption key is stored as a shared secret key on said user terminal and in a data store accessible by at least one of said application
25 servers.

12.   A method according to claim 9, 10 or 11, further comprising updating said status data for an authenticated user.

30 13.   A method according to claim 12, wherein said updating step comprises issuing a challenge to a user terminal, receiving a response to said challenge, and verifying said response.

14. A method according to claim 12 or 13, wherein said updating step is performed in response to a time-out associated with said status data.

15. A method according to claim 12 or 13, wherein said updating step is performed in response to access by one of said application servers to said status data.

16. A method according to claim 12 or 13, wherein said updating step is performed in response to a request by a user terminal.

17. A method according to any of claims 9 to 16, wherein said identifier is an IP address of the user terminal.

18. A method according to claim 9, wherein said authentication step comprises issuing said identifier to a user terminal.

19. A method according to any of claims 9 to 18, wherein said status data is stored on a storage means which said application servers are each able to access.

20. A method according to any of claims 9 to 19, wherein said authentication details include data identifying the rights of access of individual users to one or more of said application servers.

21. Apparatus for performing the steps of any preceding claim.

22. A method of transferring a file from a first client terminal to a second client terminal, said method comprising the steps of:

holding file transfer parameters for a plurality of different file transfer types;

transmitting data relating to at least one of said different file transfer types to said first and/or second client terminal; and

conducting a file transfer between said first and second client terminals in accordance with file transfer parameters stored for a selected file transfer type.

23. A method according to claim 22, comprising:

receiving said file from said first client terminal;

receiving data identifying a selected file transfer type from said first client terminal; and transmitting said file to said second client terminal in accordance with the file transfer parameters stored for said selected transfer type.

5   24.   A method according to claim 22 or 23, wherein said holding step comprises holding a list of transfer types associated with each of a plurality of user groups, and transmitting a list to said first client terminal when a user at said first client terminal is a member of the associated user group.

10   25.   A method according to claim 22, 23 or 24, wherein said file transfer parameters include a file encryption parameter, and wherein said file transfer step comprises encrypting said file during said transfer in accordance with a file encryption parameter stored for the selected file transfer type.

15   26.   A method according to claim 25, wherein said file encryption parameter indicates an embargo period for said encrypted file, and said method comprises transmitting an encryption key to said second client terminal to allow said file to be decrypted after said embargo period has expired.

20   27.   A method according to any of claims 22 to 26, wherein said file transfer parameters include a suggested storage directory for a file.

28.   A method according to any of claims 22 to 27, wherein said file transfer parameters include a file acknowledgement parameter, and said file transfer step comprises transmitting an 25   acknowledgement to said first client terminal in accordance with a file acknowledgement parameter stored for the selected file transfer type.

29.   A method according to any of claims 22 to 28, wherein said file transfer parameters include a transmission delay parameter, and said file transfer step comprises transmitting said file 30   to said second client terminal only after expiry of a delay period in accordance with a transmission delay parameter stored for said selected file transfer type.

30.   Apparatus for performing the steps of any of claims 22 to 28.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference J00024868WOA	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)

International application No. PCT/GB98/01876	International filing date *(day/month/year)* 26/06/1998	Priority date *(day/month/year)* 26/06/1997

International Patent Classification (IPC) or national classification and IPC H04L29/06

Applicant BRITISH TELECOMMUNICATIONS PUBLIC L. C. ....et al.

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 14 sheets, including this cover sheet.

   ☒ This report is also accompanied by ANNEXES, i.e. sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 4 sheets.

3. This report contains indications relating to the following items:

   I ☒ Basis of the report
   II ☐ Priority
   III ☐ Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
   IV ☒ Lack of unity of invention
   V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations suporting such statement
   VI ☐ Certain documents cited
   VII ☒ Certain defects in the international application
   VIII ☒ Certain observations on the international application

Date of submission of the demand 24/12/1998	Date of completion of this report 0 1. 10. 99
Name and mailing address of the international preliminary examining authority: European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Authorized officer Marzenke, M Telephone No. +49 89 2399 8810

Form PCT/IPEA/409 (cover sheet) (January 1994)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No. PCT/GB98/01876

I. Basis of the report

1. This report has been drawn on the basis of (*substitute sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to the report since they do not contain amendments.*):

Description, pages:

4-20	as originally filed			
1-3	as received on	14/09/1999	with letter of	10/09/1999

Claims, No.:

1-19	as received on	14/09/1999	with letter of	10/09/1999

Drawings, sheets:

1/11-11/11	as originally filed

2. The amendments have resulted in the cancellation of:

- ☐ the description, pages:
- ☐ the claims, Nos.:
- ☐ the drawings, sheets:

3. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed (Rule 70.2(c)):

4. Additional observations, if necessary:

IV. Lack of unity of invention

1. In response to the invitation to restrict or pay additional fees the applicant has:

- ☐ restricted the claims.

- ☐ paid additional fees.

- ☐ paid additional fees under protest.

☒   neither restricted nor paid additional fees.

2. ☒   This Authority found that the requirement of unity of invention is not complied and chose, according to Rule 68.1, not to invite the applicant to restrict or pay additional fees.

3. This Authority considers that the requirement of unity of invention in accordance with Rules 13.1, 13.2 and 13.3 is

□   complied with.

☒   not complied with for the following reasons:

see separate sheet

4. Consequently, the following parts of the international application were the subject of international preliminary examination in establishing this report:

□   all parts.

☒   the parts relating to claims Nos. 1-19.

V. Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes:	Claims	1-18
	No:	Claims	19
Inventive step (IS)	Yes:	Claims	1-8
	No:	Claims	9-19
Industrial applicability (IA)	Yes:	Claims	1-19
	No:	Claims	

2. Citations and explanations

see separate sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

see separate sheet

VIII. Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

    see separate sheet

IV. Lack of unity of invention

For the independent Claims 1 and 9 a lack of unity becomes apparent **a posteriori**, i.e. after taking the prior art into consideration (cf. PCT Guidelines C-III-7.5 and 7.7).

On this point, the attention of the Applicant is drawn to the fact, that the technical link between the inventions as required by Rule 13.1 PCT finds its expression in the technical relationship between those "special" technical features, as defined in Rule 13.2 PCT, that the corresponding claims produce over the prior art.

However, the subject-matter of independent claim 9 is not inventive (see section V below). Therefore the required unity of invention is not fulfilled by Claims 1 and 9 as a technical relationship involving one or more of the same or corresponding special technical features in the sense of Rule 13.2 PCT does not exist between the subject-matter of said claims.

The independent Claims 1 and 9 are thus not linked in such a way as to form a single general **inventive** concept (Rule 13.1 PCT).

V. Reasoned Statement under Article 35(2) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement

---

I

The following documents cited in the International Search Report have been considered in this report:

D1: WO 96 42041 A

D2: STAINOV R: 'Datensicherheit im Internet: Prinzipien, Möglichkeiten und Grenzen' · NTZ Nachrichtentechnische Zeitschrift, vol. 49, no. 8, 1 January 1996, pages 32-34, 36 - 38, 40

D3: US-A-5 548 646

II

1.a   General remarks

The present application relates to a method for operating an authenticating server system for authenticating users at client terminals connected via a data communications network (independent Claim 1).

Closest prior art

Document D1 discloses a method for controlling the authorization for user accesses to network servers which are located e.g. on the Internet (see Abstract; Figures 1 and 3). In D1, service requests (such as for receiving a particular hypertext document) are sent by the user's client terminal to the concerned content server including the user IP address, i.e. "an identifier" (see page 9, lines 30-33; page 11, lines 3-6).

Furthermore, D1 discloses the redirection of service requests to an authentication server which subjects the client terminal to an authentication routine by querying an account database storing authentication information such as client IP address and password (see page 12, lines 6-34; figure 3; page 14, lines 9-21; page 5, lines 24-27).

In the event that this client authentication is performed successfully, the authentication server returns a session identification "SID" to the qualified client (see page 5, lines 24- 34; page 14, lines 27-33) with which the latter obtains authorization for access within the current domain. The issued SID is then included by the client in any following service request to the content server indicating the authenticated status of the client. This status is checked by the content server through validation of the received SID before transmitting the requested document to the client (see page 6, lines 11-16; page 11, lines 3-15; page 5, lines 13-21; page 5, line 34 to page 6, line 5).

This known method possesses the disadvantage that the SID, which essentially represents a "ticket" issued by the authentication server and which is valid for a given

period of time, needs to include (i) relatively complex **self-validating** data such as e.g. a digital signature and (ii) data defining the associated expiry period.

Problem and solution of the application

The method of Claim 1 however provides (i) the storage of **status data** indicating the identifier issued to the authenticated user's terminal to be a **validated identifier** and (ii) the validation of document requests by the recipient resource, i.e. content server by **checking said status data**. In other words, the claimed method does not check the received identifier for validity but rather the associated status data.

This allows not only to associate a time-out period to the status data which is reset at each document request received for monitoring the log-on period for a user but also to issue identifiers which are not yet validated such as during an authentication procedure that allows several authentication attempts.

Further cited documents

The other documents cited in the international search report only describe a general state of the art with respect to the method in Claim 1:

Document D2 is directed to the provision of secret keys by a "key server" for data encryption between two network nodes. Document D3 describe the data encryption between network nodes by the use of intermediate "tunnelling" bridges.

Conclusion

The claimed **storage of status data that indicates an identifier's validity and that is checked** for any requests addressed to a resource server is neither disclosed nor suggested by any of the above documents. Although issuing an identifier is known per se from D1, the latter is directed to the different concept of using such an identifier as a self-contained "ticket" with an expiry date "stamped" onto it. Starting from D1, it would therefore not be obvious for the skilled person to replace such a self-validating identifier by a unique address token which is validated by checking associated status data that is external to the address token.

The subject-matter of independent Claims 1 is therefore considered to be **new** and to **involve an inventive step**, Article 33(2) and (3) PCT.

1.b   The dependent Claims 2-8 describe specific embodiments of the methods defined in the independent Claim 1 and therefore these dependent claims also fulfil the requirements of Article 33(2) and (3) PCT with respect to novelty and inventive step.

2.a   Due to its broad and vague formulation (see in particular section VIII-2.d below), the subject-matter of Claim 9 does not contain an inventive step when departing from document D1 for the following reason:

Document D1 discloses a method for controlling the authorization for user accesses to network servers (see Abstract; Figures 1 and 3). In D1, document requests are sent by the user's client terminal to the concerned content server (see page 9, lines 30-33; page 11, lines 3-6) and redirected to an authentication server which subjects the client terminal to an authentication routine by querying an account database storing authentication details (see page 12, lines 6-34; figure 3; page 14, lines 9-21; page 5, lines 24-27).

The authentication server generates a session identification "SID" (i.e. "status data distinguishing said user from other users which are not currently authenticated") (see page 5, lines 24-34; page 14, lines 27-33) and returns this "SID" to the client. The issued SID is then included by the client in any following service request to the content server indicating the authenticated status of the client. This status is checked by the content server before transmitting the requested document to the client by validating the received SID (see page 6, lines 11-16; page 11, lines 3-15; page 5, lines 13-21; page 5, line 34 to page 6, line 5).

Therefore, the subject-matter of Claim 9 differs from the disclosure of D1 in that the claimed method further provides the generation and storage of a secret key shared between the resource server and the user for secure data communications.

This general feature and its underlying technical problem of securing data communications are however largely known to the skilled person in the field of

telecommunications as can be seen e.g. from document D2 (see page 37, figure 4; page 36, right column "Geheime symmetrische Schlüssel" to page 38, end of left column).

Consequently, the subject-matter of Claim 9 does not contain an inventive step and Claim 9 thus does not meet the requirements of Article 33(1) and (3) PCT.

2.b   The additional features of the dependent Claims 10-18, are either directly derivable from the above cited documents or concern simple embodiments without inventive merit in themselves. These claims do not, therefore, add inventive matter to the claims upon which they are dependent and, as a consequence, do not meet the requirements of Articles 33(1) and (3) PCT.

3.   The independent system Claim 19 does not contain any features defining any of its constituent means (see section VIII below). As Claim 19 merely indicates that the system is **suitable** for performing any of the previously defined methods, Claim 19 fails to provide any technical means that would distinguish its subject-matter from the system used in D1 for user access control. The system of Claim 19 **per se** is in fact known from D1 (see e.g. figures 1 and 3).

Consequently, the subject-matter of Claim 19 is not novel and Claim 19 therefore does not meet the requirements of Article 33(1) and (2) PCT.

VII.   Certain defects in the international application

1.   To meet the requirements of Rule 6.3(b) PCT the independent claims should be cast in the two-part form, with those features known in combination from the prior art (see document D1) being placed in a preamble (Rule 6.3(b)(i) PCT) and with the remaining features being included in a characterising part (Rule 6.3(b)(ii) PCT).

2.   To fulfil the requirements of Rule 5.1(a)(ii) PCT, documents D2 to D3 should be

identified in the description and the relevant background art disclosed therein briefly discussed.

3.   The opening part of the description should be brought into conformity with any amended independent claims (Rule 5.1(a)(iii) PCT).

4.   Furthermore, following the disclosure of document D1, the statement indicating the technical problem to be solved by the invention, requires revision, which should be effected taking the requirements of Rule 5.1(a)(iii) PCT into account.

5.   Reference signs placed in parentheses should be inserted into all the claims to increase their intelligibility (Rule 6.2(b) PCT). This applies to both the preamble and the characterising portion.

VIII. Certain observations on the international application

1.   The subject-matter of independent method Claim 1 is not clear (Article 6 PCT) for the following reasons:

    a.   The present broad formulation (see page 21, line 7: "storing authentication details of authorised users") does not define **where** the authentication details are stored within the server system. Consequently it is not clear, how the subsequent method step of "validating said authentication data by reference to said stored authentication details" (see page 21, lines 9-10) is performed.

    b.   The formulation "**by reference** to said stored authentication details" (see page 21, lines 9-10) is ambiguous as it fails to clearly define the method steps necessary to perform the user authentication in connection with the stored authentication details. In other words, it is not clear, which **functional** link exists between the user authentication and the stored details.

        This is further corroborated by the fact that neither the "authentication details" nor the "authentication data" have been previously defined as to any of their

technical characteristics. It is in fact not clear, whether these terms refer to the user's password and username or to the challenge/response value pair all of which are being used for the authentication procedure.

c. The formulation of Claim 1 does not define at all the location of the claimed "authentication server system" and "resource server" (see page 21, lines 3 and 5) in relation to the client terminals and the data communications network. Therefore, it is not understood from the wording of the claim,

   i. if at all and how the authenticating server system intervenes in the subsequently claimed authentication and document request stages;
   ii. how, i.e. via which connection, the document requests are directed from the client terminal to the resource server.

d. The term **"enabling** said resource server to validate a request" leaves the reader in doubt as to whether the step of validating the request by the resource server forms actually part of the scope for which protection is sought.

e. The present formulation "issuing an identifier for the user's terminal **to said terminal** for storage thereon, the identifier being transmitted **in such a manner** that the identifier is retransmitted **by said user terminal**" (see page 21, lines 11-13) is ambiguous as it seeks to incorporate two functionally different method steps into one:

   i. transmission of an identifier **to the user terminal** for storage thereon; and
   ii. transmission of the stored identifier **by the user terminal** in document requests directed to said resource server.

This is corroborated by the fact, that it is indeed not understood, how the first of these transmissions functionally affects the second of these transmissions as implied by the above formulation "*in such a manner*".

f. The inconsistent formulation of Claim 1 (see page 21, lines 11 and 12) leaves the reader in doubt as to whether the "issuing" and the "transmitting" of the identifier define in fact the same method step performed on the identifier or, if

not, how the "issuing" and the "transmitting" actually differ in technical terms.

g.   Neither "said authentication step" nor "said document request" as presented in Claim 1 (see page 21, lines 16 and 20) have been previously defined.

2.   The subject-matter of independent method Claim 9 is not clear (Article 6 PCT) for the following reasons:

a.   The objections raised in paragraph 1-a and 1-c above apply equally to method Claim 9 (see page 22, lines 25-27).

b.   Claim 9 refers to "the user's terminal" (see page 22, line 32) which has not previously been defined anywhere in the claim.

c.   The vague term "**accessible**" (see page 22, line 30 and page 23, line 1) leaves the reader in doubt as to whether the access storage means for the status data and the shared secret key by the resource server(s) is in fact part of the claimed method or not, rendering the scope for which protection is sought obscure.

d.   The vague formulation of Claim 9 (see page 22, lines 30-32: "storing said status data in storage means accessible to said plurality of resource servers to check an authentication status of said user by using an identifier for the user's terminal received in a service request") is ambiguous. In fact, it is not clear for the reader whether the authentication status of said user is checked:

i.   with the help of the storage means; or
ii.   by using an identifier for the user's terminal; or
iii.   by a combination of i and ii.

Furthermore, Claim 9 does not specify for the cases ii and iii above, how the identifier is "used" for checking the authentication status of said user if not in the manner described in document D1.

By comparison to the features of independent Claim 1 (see in particular page

21, lines 15-16), it seems that the aforementioned ambiguity in Claim 9 is caused by the fact, that the subject-matter of Claim 9 is silent about the essential technical link between the status data and the identifier, namely that the status data indicates the identifier to be a validated identifier of a terminal of a currently authenticated user. It is indeed through this feature that the authentication status of a user can be verified by checking the associated status data for an identifier included in a service request.

Independent method Claim 9 therefore does also not meet the requirement following from Article 6 PCT taken in combination with Rule 6.3(b) PCT, that any independent claim must contain all the technical features essential to the definition of the invention.

3.   Despite its reference to previous claims, the apparatus Claim 19 has to be considered independent, since it claims an authenticating server system and not a method of operating an authenticating server system as is the case for all the previous method claims.

As already explained in the invitation to restrict or pay additional fees dated 28.4.99 and in the written opinion dated 25.6.99, it is reiterated that a claim may contain a reference to another claim without necessarily being a dependent claim (see PCT, chapter III-3.7a). In particular, a claim referring to a claim of another category (such as an apparatus claim referring to a method claim) is, per definition, an independent claim.

The fact that Claim 21 refers to the previous method claims simply means that the apparatus is **suitable** for being used to perform such methods, without necessarily defining the means which are required (see also PCT Guidelines, chapter III-4.8).

One can indeed construe an indefinite number of server systems which all perform the claimed methods but which possess different internal architectures.

Therefore, even when including the reference to the previous method claims, Claim 19 does not contain all the essential features necessary to define the invention as

required by Article 6 PCT in combination with Rule 6.3(b) PCT.

4. Concerning the dependent claims, the following objections with respect to Article 6 PCT are raised:

    i.   Claims 3 and 4 refer to "said authentication step" (see page 21, lines 25 and 29) which has not been previously defined.

    ii.   Concerning Claims 5 and 6, it is not clear whether the term "authenticator(s)" as presented in these claims refers in fact to the identifier included in a document request sent by a user terminal or not. In case this term is supposed to define another authentication token than the aforementioned identifier, the technical significance of such authenticators is however not clear from the wording of these claims.

    iii.   Claims 10 and 14-16 refer to "the user's terminal" (see page 23, lines 5, 18, 21 and 24) which has not been previously defined.

    iv.   Claim 11 refers to "said storing step" (see page 23, line 9) leaving the reader in doubt as to which of the two storing steps as defined in Claim 9 is referred to by this term.

    v.   Claim 18 refers to "said application servers" (see page 23, line 31) which has not been previously defined.